brother

IPsec 設定ガイド

Version 0

JPN

マークについて

本文中では、マークについて、次のように表記しています。

メモ	知っていると便利なことや、補足を記載しています。

商標について

Brother ロゴはブラザー工業株式会社の登録商標です。

ブラザー製品および関連資料等に記載されている社名及び商品名はそれぞれ各社の商標または登録商標です。

目次

1 はじめに

概要

IPsec（Internet Protocol Security）は、IP プロトコルのオプション機能で、IP パケット単位でデータの改ざん防止や、秘匿機能を提供するセキュリティプロトコルです。本機能はネットワーク上をいきかうデータ、例えばパソコンからプリンターに送られる印刷データ等を、IPsec を使用して暗号化します。ネットワーク層で暗号化を行うため、その上位のプロトコルを利用するアプリケーションソフトは、IPsec を意識する必要なく IPsec を利用することができます。

IPsec は次の機能をサポートしています。

■ IPsec 送受信

IPsec の設定条件に従い、ネットワークに接続されたパソコンが、指定された相手と IPsec によるデータ通信を行います。IPsec による通信を開始すると、まず IKE（Internet Key Exchange）により鍵交換が実施され、IKE で得た鍵により、暗号化されたデータの通信が行われます。
また、IPsec は、トランスポートモード・トンネルモードの 2 つの動作モードを持ち、トランスポートモードは主にデバイス間通信で使用され、トンネルモードは、VPN（Virtual Private Network）などの環境で使用されます。

メモ

- IPsec 送受信を行うには、以下の条件が必要です。
  - IPsec 通信可能なパソコンがネットワーク上に接続されていること。
  - プリンターまたは複合機に、IPsec の設定がされていること。
  - プリンターまたは複合機と接続するパソコンに、IPsec 接続可能な設定がされていること。
- ブロードキャスト、マルチキャスト通信では、IPsec はサポートされません。

■ IPsec 設定

IPsec 接続に必要な設定を行います。IPsec 設定は、ウェブブラウザー（Web Based Management）を使用して設定することができます。（「ウェブブラウザー（Web Based Management）を使った設定方法」（2 ページ））をご覧ください。

メモ

IPsec 設定を行うには、ウェブブラウザーが動作可能なパソコンが LAN で接続されている必要があります。

ウェブブラウザー（Web Based Management）を使った設定方法

ウェブブラウザーの IPsec 設定画面で IPsec 接続条件を設定します。

IPsec 接続条件は、アドレス、サービス、**IPsec** の 3 つのテンプレートで構成され、最大 10 個の接続条件が設定可能です。

1. ウェブブラウザーを起動します。
2. ウェブブラウザーのアドレス入力欄に、“http:// 本製品の IP アドレス /” と入力します。
   - 例：

     http://192.168.1.2/
3. お買い上げ時の設定では、パスワードは必要ありません。パスワードを設定している場合は、パスワードを入力し、を押します。
4. ネットワークタブをクリックします。
5. セキュリティをクリックします。
6. **IPsec** をクリックします。
7. 以下の画面から IPsec 設定ができます。

- **状態**

  IPsec の**有効**または**無効**を設定します。

- **接続モード**

  IKE Phase1 のモードを設定します。

  - メイン：メインモードを使用します。
  - アグレッシブ：アグレッシブモードを使用します。

メモ

IKE は、IPsec を使って暗号化通信を行うための暗号鍵交換に利用するプロトコルです。

メインモードを選ぶと、処理速度は遅くなりますが、安全性は高くなります。アグレッシブモードを選ぶと、メインモードより処理速度が速くなりますが、セキュリティは低下します。

- **IPsec 以外のトラフィックルール**

  非 IPsec パケットの扱いを設定します。

  - **通過**：全てのパケット受信を許可します。
  - **遮断**：非 IPsec パケットを破棄します。

メモ

Web Services を使用する場合は、**IPsec 以外のトラフィックルール**を**通過**に設定してください。**遮断**を選択すると、Web Services を使用することはできません。

- **ルール**

  IPsec の接続条件（テンプレート）を、10 個まで設定できます。

- **有効**

  選択した番号のテンプレートを有効にします。

メモ

複数のチェックボックスを選択し、それらの設定が互いに矛盾する場合は、早い番号のものが優先されます。

- **テンプレート - アドレス**

  IPsec 接続条件となるアドレステンプレートを選択します。

  アドレステンプレートを追加するときは、**テンプレートの追加**をクリックします。（「アドレステンプレート」（5 ページ））をご覧ください。

- **テンプレート - サービス**

  IPsec 接続条件となるサービステンプレートを選択します。

  サービステンプレートを追加するときは、**テンプレートの追加**をクリックします。（「サービステンプレート」（7 ページ））をご覧ください。

メモ

付録 A に記載されているサービステンプレート 2、3、4 を使用したときに、DNS で名前解決をしたい場合は、別途 DNS の設定が必要です。

- テンプレート - **IPsec**

  IPsec 接続条件となる **IPsec** テンプレートを選択します。

  IPsec テンプレートを追加するときは、**テンプレートの追加**をクリックします。（「IPsec テンプレート」（12 ページ））をご覧ください。

- **OK**

  設定値を登録します。設定の変更のために再起動が必要な場合は、再起動確認画面が表示されます。

メモ

有効にチェックを入れて **OK** をクリックしたとき、テンプレート内に空欄があると、エラーになります。

2 IPsec 設定

アドレステンプレート

IPsec 接続条件となる IP アドレスの設定を行います。アドレステンプレートは 10 個まで設定できます。

1. ウェブブラウザーを起動します。
2. ウェブブラウザーのアドレス入力欄に、“http:// 本製品の IP アドレス /” と入力します。
   - 例：

     http://192.168.1.2/
3. お買い上げ時の設定では、パスワードは必要ありません。パスワードを設定している場合は、パスワードを入力し、→を押します。
4. ネットワークタブをクリックします。
5. セキュリティをクリックします。
6. **IPsec** アドレステンプレートをクリックします。
   アドレステンプレートが 10 個表示されます。アドレステンプレートが未設定時は、**未登録**と表示されます。
   - **削除**

     アドレステンプレートを削除します。現在使用されているアドレステンプレートは、削除できません。
7. 作成したい番号のアドレステンプレートをクリックします。以下の画面で IPsec を実行したい IP アドレスを設定して、**IPsec** アドレステンプレートを作成します。

- テンプレート名

  作成するテンプレート名を入力します。（最大 16 文字）

- ローカル **IP** アドレス

  発信元の IP アドレス条件を設定します。

  - **IP** アドレス

    IP アドレスを設定します。すべての **IPv4** アドレス、すべての **IPv6** アドレス、すべてのリンクローカル **IPv6** アドレス、カスタムから選択できます。カスタムを選択した場合は、特定の IP アドレス（IPv4 または IPv6）をテキストボックスに入力します。

  - **IP** アドレス範囲

    IP アドレス範囲の始点と終点を入力します。始点と終点が IPv4 か IPv6 で統一されていない場合や、始点より小さいアドレスを終点に入力した場合は、エラーとなります。

  - **IP** アドレス **/** プレフィックス

    プレフィックスを使って、IP アドレスを設定します。

    例：192.168.1.1/24

    192.168.1.1 に対し 24bit のサブネットマスク（255.255.255.0）となり、192.168.1.xx が有効となります。

- リモート **IP** アドレス

  宛先の IP アドレス条件を設定します。

  - すべて

    全ての IP アドレスを許可します。

  - **IP** アドレス

    特定の IP アドレス（IPv4 または IPv6）をテキストボックスに入力します。

  - **IP** アドレス範囲

    IP アドレス範囲の始点と終点を入力します。始点と終点が IPv4 か IPv6 で統一されていない場合や、始点より小さいアドレスを終点に入力した場合は、エラーとなります。

  - **IP** アドレス **/** プレフィックス

    プレフィックスを使って、IP アドレスを設定します。

    例：192.168.1.1/24

    192.168.1.1 に対し 24bit のサブネットマスク（255.255.255.0）となり、192.168.1.xx が有効となります。

- **OK**

  設定値を登録します

メモ

使用中のテンプレートを変更した場合は、ウェブブラウザーの IPsec 設定画面が再起動します。

サービステンプレート

IPsec サービステンプレート

IPsec 接続を行うプロトコルおよびポート番号を設定します。サービステンプレートは 10 個まで設定できます。

1. ウェブブラウザーを起動します。
2. ウェブブラウザーのアドレス入力欄に、“http:// 本製品の IP アドレス /” と入力します。
   - 例：

     http://192.168.1.2/
3. お買い上げ時の設定では、パスワードは必要ありません。パスワードを設定している場合は、パスワードを入力し、→を押します。
4. ネットワークタブをクリックします。
5. セキュリティをクリックします。
6. **IPsec** サービステンプレートをクリックします。
   サービステンプレートが 10 個表示されます。サービステンプレートが未設定時は、**未登録**と表示されます。
   - **削除**

     サービステンプレートを削除します。現在使用されているサービステンプレートは、削除できません。
7. 作成したい番号のサービステンプレートをクリックします。以下の画面で IPsec を実行したいサービスを選択して、**IPsec** サービステンプレートを作成します。
   また、新規にサービスを作成したい場合は、**サービス設定**をクリックしてください。(「サービス設定」(8 ページ)) をご覧ください。

■ テンプレート名

作成するテンプレート名を入力します。(最大 16 文字)

■ サービス名

デフォルトと作成済みのサービス名が表示されます。テンプレートに追加したいサービスを選択してください。

■ サービス設定

クリックすると、サービスを追加することができます。(「サービス設定」(8 ページ))をご覧ください。

■ 選択されたサービス

サービス名で選択したサービスの内容(**サービス名**、**方向**、**プロトコル**、**ポート**)を表示します。

メモ

- 一度に設定できるサービスの数は 32 個までです。
- **IPsec** サービステンプレートで使用できるプロトコルの詳細については、付録 A をご覧ください。

■ **OK**

設定値を登録します。

メモ

使用中のテンプレートを変更した場合は、ウェブブラウザーの **IPsec** 設定画面が再起動します。

サービス設定

新しいサービスを作成します。

1. **IPsec** サービステンプレート画面で、**サービス設定**をクリックします。
サービス名が 60 個表示されます。**サービス名**が未設定時は**未登録**と表示されます。

■ 削除

サービス名を削除します。現在使用されている**サービス名**は、削除できません。

■ **IPsec** サービステンプレート

IPsec サービステンプレート画面に戻ります。

2 作成したい番号の**サービス名**をクリックします。以下の画面で IPsec を実行したいサービスを設定してください。プロトコルの選択内容によって、設定項目が切り替わります。

(プロトコル：**ALL**)

(プロトコル：**TCP** または **UDP**)

（プロトコル：**ICMP**）

■ サービス名

作成するサービス名を入力します。（最大 16 文字）

■ 方向

通信の方向を設定します。**Initiator**、**Responder**、**Both** から選択してください。

■ プロトコル

有効にするプロトコルを設定します。**ALL**、**TCP**、**UDP**、**ICMP** から選択してください。選択したプロトコルによって、以降の設定項目が切り替わります。

- **TCP** または **UDP** 選択時、**送信元ポート**と**宛先ポート**を登録します。
- **ICMP** 選択時、タイプとコードを登録します。

メモ

ICMP は、IP のエラーメッセージや制御メッセージを転送するプロトコルです。TCP/IP で接続されたパソコンやネットワーク機器間で、互いの状態を確認するために用いられます。

■ **送信元ポート / 宛先ポート**（プロトコルで **TCP** または **UDP** 選択時）

送信元ポート No. を入力します。シングルを選択した場合は、ポート No. をひとつ入力し、**範囲指定**を選択した場合は、ポート No. の始点、終点の順に入力してください。

全てのポートを許可したい場合は、**範囲指定**を選び 1 ～ 65,535 を入力してください。

■ **ICMP**（ローカル）/**ICMP**（リモート）（プロトコルで **ICMP** 選択時）

ICMP の詳細を設定します。**すべて**を選択するか、タイプとコードを入力してください。タイプとコードの詳細については、付録 A をご覧ください。

■ **サービス設定**

サービス設定画面に戻ります。

- **OK**

  設定値を登録します

使用中のテンプレートを変更した場合は、ウェブブラウザーの IPsec 設定画面が再起動します。

IPsec テンプレート

IKE/IPsec の設定をします。**IPsec** テンプレートは 10 個まで設定できます。

1 ウェブブラウザーを起動します。

2 ウェブブラウザーのアドレス入力欄に、“http:// 本製品の IP アドレス /” と入力します。
   - 例：

     http://192.168.1.2/

3 お買い上げ時の設定では、パスワードは必要ありません。パスワードを設定している場合は、パスワードを入力し、➔を押します。

4 ネットワークタブをクリックします。

5 セキュリティをクリックします。

6 **IPsec** テンプレートをクリックします。
IPsec テンプレートが 10 個表示されます。**IPsec** テンプレートが未設定時は、**未登録**と表示されます。
   - 削除

     IPsec テンプレートを削除します。現在使用されている **IPsec** テンプレートは、削除できません。

7 作成したい番号の **IPsec** テンプレートをクリックします。以下の画面で IPsec の設定を行い、**IPsec** テンプレートを作成します。テンプレートを使用する、**IKE** の選択内容によって、設定項目が切り替わります。

（**IKE**：プリセット）

（**IKE**：**IKEv1**）

（**IKE：IKEv2**）

■ テンプレート名

作成するテンプレート名を入力します。（最大 16 文字）

■ テンプレートを使用する

カスタム、**IKEv1** 高セキュリティ、**IKEv1** 中セキュリティ、**IKEv2** 高セキュリティ、**IKEv2** 中セキュリティから選択してください。ここで選択したテンプレートによって、以下の項目が切り替わります。

メモ

IPsec 画面の接続モードで選択している内容によって、デフォルトテンプレートの内容が変わります。IPsec 画面については「ウェブブラウザー（Web Based Management）を使った設定方法」（2 ページ）をご覧ください。

■ **IKE**

IPsec で暗号化通信を行う際に、暗号鍵を交換するために利用される通信プロトコルです。その場限りの暗号化通信を行って、IPsec に必要な暗号化アルゴリズムの決定と暗号鍵の共有を行います。IKE では Diffie-Hellman 鍵交換と呼ばれる手順によって暗号鍵を交換し、IKE 限定の暗号化通信を行います。

テンプレートを使用するでカスタムを選択した場合は、**IKEv1**、**IKEv2**、**手動**から選択してください。

カスタム以外を選択した場合は、テンプレートを使用するで選択した設定が表示されます。

■ 認証タイプ

IKE の認証 / 暗号化の設定をおこないます。

- **DH** グループ

  安全でない通信経路を使って秘密鍵を安全に送受信するための鍵交換方式です。Diffie-Hellman 鍵交換では、離散対数問題を利用して、秘密鍵そのものではなく、乱数と秘密鍵から生成した公開情報を送受信します。

  (テンプレートを使用するでカスタム、**IKE** で **IKEv1** または **IKEv2** 選択時) グループ **1**、グループ **2**、グループ **5**、グループ **14** から選択してください。**IKEv2** を選択した場合は、複数設定が可能です。

  (テンプレートを使用するでカスタム、**IKE** で手動選択時) 表示されません。

  (テンプレートを使用するでカスタム以外を選択時) 上記のうち有効なグループが表示されます。

- 暗号化方式

  (テンプレートを使用するでカスタム、**IKE** で **IKEv1** または **IKEv2** 選択時) **DES**、**3DES**、**AES-CBC 128**、**AES-CBC 256** から選択してください。**IKEv2** を選択した場合は、複数設定が可能です。

  (テンプレートを使用するでカスタム、**IKE** で手動選択時) 表示されません。

  (テンプレートを使用するでカスタム以外を選択時) 上記のうち有効な暗号化方式が表示されます。

- ハッシュ

  (テンプレートを使用するでカスタム、**IKE** で **IKEv1** または **IKEv2** 選択時) **MD5**、**SHA1**、**SHA256**、**SHA512** から選択してください。**IKEv2** を選択した場合は、複数設定が可能です。

  (テンプレートを使用するでカスタム、**IKE** で手動選択時) 表示されません。

  (テンプレートを使用するでカスタム以外を選択時) 上記のうち有効なハッシュが表示されます。

- **SA** ライフタイム

  IKE SA のライフタイムを設定します。

  (テンプレートを使用するでカスタム、**IKE** で **IKEv1** または **IKEv2** 選択時) 時間 (秒) と量 (KB) で入力してください。

  (テンプレートを使用するでカスタム、**IKE** で手動選択時) 表示されません。

  (テンプレートを使用するでカスタム以外を選択時) 時間 (秒) と量 (KB) で表示されます。

■ 動作セキュリティ

- プロトコル

  (テンプレートを使用するでカスタム選択時) **ESP** または **AH** から選択してください。**IKE** が **IKEv2** の場合は、**ESP** のみ選択可能です。

  (テンプレートを使用するでカスタム以外を選択時) 上記のうち有効なプロトコルが表示されます。

メモ

- ESP は、IPsec による暗号化通信で送受信される、ペイロード（通信内容）を暗号化して付加情報を足したものです。IP パケットのヘッダ部に続くペイロード部を暗号化したもので、暗号化されたデータ本体に一定の形式で暗号化方式や鍵についての情報、認証データなどが付与された構造になっています。
- AH は、IPsec の仕様の一部で、送信元の認証や改ざん防止（完全性の保証）を実現するための仕組みです。IP パケットの中でヘッダの直後に挿入されるデータで、通信内容や秘密鍵などから一定の計算によって割り出したハッシュ値を含み、これにより送信元の偽証や通信内容の改ざんを防止します。ESP と異なり通信内容の暗号化は行わず、データ本体は平文で送受信されます。

2

- 暗号化方式

  （テンプレートを使用するでカスタム選択時）**DES**、**3DES**、**AES-CBC 128**、**AES-CBC 256** から選択してください。プロトコルが **ESP** の場合のみ選択可能です。**IKE** が **IKEv2** の場合は、複数設定が可能です。

  （テンプレートを使用するでカスタム以外を選択時）上記のうち有効な暗号化方式が表示されます。

- ハッシュ

  （テンプレートを使用するでカスタム、**IKE** で **IKEv1** または 手動選択時）なし、**MD5**、**SHA1**、**SHA256**、**SHA512** から選択してください。なしはプロトコルが **ESP** の場合のみ選択可能です。

  （テンプレートを使用するでカスタム、**IKE** で **IKEv2** 選択時）**MD5**、**SHA1**、**SHA256**、**SHA512** から選択してください。複数設定が可能です。

  （テンプレートを使用するでカスタム以外を選択時）上記のうち有効なハッシュが表示されます。

- **SA** ライフタイム

  IKE SA のライフタイムを設定します。

  （テンプレートを使用するでカスタム、**IKE** で **IKEv1** または **IKEv2** 選択時）時間（秒）と量（KB）で入力してください。

  （テンプレートを使用するでカスタム以外を選択時）時間（秒）と量（KB）で表示されます。

- 動作モード

  トランスポートまたはトンネルから選択してください。

- リモートルーター **IP** アドレス

  接続先ルータの IP アドレス（IPv4 または IPv6）を設定します。トンネルモード選択時のみ入力してください。

メモ

SA（Security Association）とは、IPsec や IPv6 を利用した暗号化通信において、通信をはじめる前に暗号化方式や暗号鍵などの情報を交換・共有し、安全な通信路を確立することです。確立された仮想的な暗号通信路のことを指す場合もあります。IPsec における SA では、IKE（Internet Key Exchange）という標準手順によって、暗号化方式の決定や鍵の交換、相互の認証がおこなわれ、SA は定期的に更新されます。

- **PFS**

  PFS は、メッセージの暗号化に使った鍵で、別の鍵を作りません。また、メッセージの暗号化に使われている鍵があるときに、その鍵を作った親鍵で別の鍵を作りません。このため、ある鍵を知られてしまっても、その鍵で暗号化したメッセージ以外に被害が及ぶことはありません。

  有効または**無効**から選択してください。**テンプレートを使用する**で**カスタム**、**IKE** で**手動**を選択した場合は、PFS は表示されません。

- **認証方式**

  認証方式を選択します。**事前共有キー**、**証明書**、**EAP-MD5**、**EAP-MS-CHAPv2** から選択してください。

  EAP-MD5、**EAP-MS-CHAPv2** は **IKE** が **IKEv2** の場合のみ選択可能です。**テンプレートを使用する**で**カスタム**、**IKE** で**手動**を選択した場合は、認証方式は表示されません。

- **事前共有キー**

  通信を暗号化する際に、事前に別の手段で暗号鍵を交換して共有しておきます。

  認証方式で**事前共有キー**を選択した場合は、**事前共有キー**を入力してください。（最大 32 文字）

  - ローカル **ID** タイプ **/ID**

    発信元 ID のタイプを選択し、ID を入力します。

    タイプは **IPv4** アドレス、**IPv6** アドレス、**FQDN**、**E-mail** アドレス、**証明書**から選択してください。

    証明書を選択した場合は、**ID** に証明書のコモンネームを入力してください。

  - リモート **ID** タイプ **/ID**

    宛先 ID のタイプを選択し、ID を入力します。

    タイプは **IPv4** アドレス、**IPv6** アドレス、**FQDN**、**E-mail** アドレス、**証明書**から選択してください。

    証明書を選択した場合は、**ID** に証明書のコモンネームを入力してください。

- **証明書**

  認証方式で**証明書**を選択した場合は、証明書を選択します。

選択できる証明書は、ウェブブラウザー（Web Based Management）のセキュリティー設定の**証明書**ページで登録されているものだけです。詳細については、➤➤ ユーザーズガイド ネットワーク編「本製品を安全に管理するために証明書を使用する」をご覧ください。

■ **EAP**

PPP を拡張した認証プロトコルで、IEEE802.1x とともに使うことにより、ユーザー認証とセッションごとに異なった鍵を運用します。

認証方式で **EAP-MD5** または **EAP-MS-CHAPv2** を選択している場合のみ、以下の設定が必要です。

- モード

  サーバーモード、クライアントモードから選択してください。

- 証明書

  証明書を選択してください。

- ユーザー名

  ユーザーネームを入力してください。（最大 32 文字）

- パスワード

  パスワードを入力してください。確認用に 2 回入力が必要です。（最大 32 文字）

- 証明書 >>

  証明書設定画面に移動します。

（**IKE**：手動）

■ 認証キー（**ESP, AH**）

認証で使用するキーを設定します。**In** と **Out** に入力してください。

テンプレートを使用するでカスタム、**IKE** で手動を選択し、動作セキュリティのハッシュでなし以外を選択した場合は、設定が必要です。

メモ

動作セキュリティのハッシュで選択している値によって、設定できる文字数が異なります。選択しているハッシュアルゴリズムの長さと一致しない場合は、エラーとなります。

- **MD5**：128bit （16Byte）
- **SHA1**：160bit （20Byte）
- **SHA256**：256bit （32Byte）
- **SHA512**：512bit （64Byte）

アスキーコードで入力する際は、文字をダブルクォーテーション（"）で囲んでください。

■ コードキー（**ESP**）

暗号で使用するキーを設定します。**In** と **Out** に入力してください。

テンプレートを使用するでカスタム、**IKE** で手動、動作セキュリティのプロトコルで **ESP** を選択した場合は、設定が必要です。

メモ

動作セキュリティの暗号化方式で選択している値によって、設定できる文字数が異なります。選択している暗号化方式アルゴリズムの長さと一致しない場合は、エラーとなります。

- **DES**：64bit （8Byte）
- **3DES**：192bit （24Byte）
- **AES-CBC 128**：128bit （16Byte）
- **AES-CBC 256**：256bit （32Byte）

アスキーコードで入力する際は、文字をダブルクォーテーション（"）で囲んでください。

- **SPI**

  セキュリティ情報を識別するためのパラメーター（値）です。一般に、1 つのホストは複数の IPsec の通信に対応する複数の SA（Security Association）を持つため、受け取った IPsec のパケットがどの SA に対応するものかを識別する必要があります。これを示すパラメーター（値）が、AH（Authentication Header）や ESP（Encapsulating Security Payload）のヘッダ内に含まれる SPI です。

  テンプレートを使用するでカスタム、**IKE** で手動を選択した場合は、設定が必要です。

  In と **Out** に入力してください。（3 ～ 10 文字）

- **OK**

  設定値を登録します。

メモ

使用中のテンプレートを変更した場合は、ウェブブラウザーの IPsec 設定画面が再起動します。

付録 A

サービステンプレート

テンプレートを選択すると、以下のサービスを利用することができます。

1 すべてのサービス

すべてのプロトコルに対して IPsec をかけます。

2 印刷サービス

サービス名	プロトコル	送信元ポート	宛先ポート
IPP	TCP	631	すべて
IPPS	TCP	443	すべて
FTP （コントロール）	TCP	21	すべて
FTP （データ）	TCP	20	すべて
P9100	TCP	9100	すべて
Web Services	TCP	80	すべて
LPD	TCP	515	すべて

3 管理サービス

サービス名	プロトコル	送信元ポート	宛先ポート
SNMP	UDP	161	すべて
Telnet	TCP	23	すべて
HTTP	TCP	80	すべて
HTTPS	TCP	443	すべて
リモートセットアップ	TCP	54922	すべて

4 プリンター /MFC サービス [1]

サービス名	プロトコル	送信元ポート	宛先ポート
CIFS	TCP	すべて	445
SMB	TCP	すべて	139
LDAP	TCP	すべて	389
SMTP	TCP	すべて	25
POP3	TCP	すべて	110
SNTP	UDP	すべて	123
Network Scan	TCP	54921	すべて
PC-FAX	TCP	54923	すべて
Kerberos 認証（TCP）	TCP	すべて	88
Kerberos 認証（UDP）	UDP	すべて	88

[1] Kerberos 認証を利用したい場合は、適宜 DNS を有効に設定する必要があります。

タイプ / コード

プロトコルに ICM を設定している場合は、以下のタイプとコードをサポートします。

IPv4		
タイプ		対応コード
0	Echo Reply	0
3	Destination Unreachable	0,1,2,3,4,5,6,7,8,9,10,11,12
4	Source Quench	0
5	Redirect	0,1,2,3
8	Echo Request	0
9	Router Advertisement	0
10	Router Solicitations	0

IPv4 コード

0,1,2,3,4,5,6,7,8,9,10,11,12

IPv6		
タイプ		対応コード
1	Destination Unreachable	0,1,2,3,4
3	Time Exceeded	0,1
4	Parameter Problem	0,1,2
128	Echo Request	0
129	Echo Reply	0
133	Router Solicitation	0
134	Router Advertisement	0
135	Neighbor Solicitation	0
136	Neighbor Advertisement	0
137	Redirect	0

IPv6 コード

0,1,2,3,4